EXAMINER'S AMENDMENT

1. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

2. Authorization for this examiner's amendment was given in a telephone interview with the applicant representative, Mr. George H. Gates (Reg. No. 33,500) on 11/18/09. During the telephone conference, Mr. Gates has agreed and authorized examiner to amend claims 17, 46 to distinguish over the prior arts of record, claims 1, 17 to overcome the 101 issue and claims 31-45, 47-58 to overcome the 112 issue.

3. Regarding to the information disclosure statement filed April 6, 2004: NPL documents C1, C2, C7, C21, C23, C26, C32, C33-C35 have not been considered because they do not have date information, which is confirmed with Mr. Gates on 11/30/09.

CLAIMS:

a. Referring to claim 1:

Please replace claim 1 as follows:

A computer-implemented method for processing data comprising:

(a) performing, in a computer, an enrollment process, comprising:

receiving a first biometric data and a first personal key;

processing the first biometric data combined with the first personal key through an irreversible cryptographic algorithm executed by the computer to form a first processed data comprised of the first biometric data and the first personal key in an irreversibly encrypted form;

eliminating all storage or trace of the first biometric data and the first personal key in an unprocessed and unencrypted form after the first processed data has been formed and prior to any storage; and

storing the first processed data in a repository for use in a subsequent authentication process; and

(b) performing, in a computer, an authentication process, comprising:

receiving a second biometric data and a second personal key;

processing the second biometric data combined with the second personal key through the irreversible cryptographic algorithm executed by the computer to form a second processed data comprised of the second biometric data and the second personal key in an irreversibly encrypted form;

eliminating all storage or trace of the second biometric data and the second personal key in an unprocessed and unencrypted form after the second processed data has been formed and prior to any comparison;

comparing the second processed data to the first processed data previously stored in the repository, without accessing either the first or second processed data in an unprocessed and unencrypted form, in order

to enable authentication of the second biometric data and the second personal key in a confidential manner; and

generating a signal pertaining to the comparison of the second processed data to the first processed data for use in the authentication process.

b. Referring to claim 17:

Please replace claim 17 as follows:

A computer-implemented method for processing data comprising:

receiving biometric data and a personal key;

processing the biometric data combined with the personal key through an irreversible cryptographic algorithm executed by a computer to form a processed data comprised of the biometric data and the personal key in an irreversibly encrypted form;

eliminating all storage or trace of the biometric data and personal key in an unprocessed and unencrypted form prior to any comparison; and

comparing the processed data to secondary data stored in a repository, without accessing the processed data in an unprocessed and unencrypted form, in order to enable authentication of the biometric data and personal key in a confidential manner ;

wherein the secondary data comprises one or more combinations of biometric data and personal keys stored in the repository in an irreversibly encrypted form during an enrollment process that processes the one or more combinations of biometric data and personal keys through an irreversible cryptographic algorithm executed by a

computer to form the secondary data, eliminates all storage or trace of the one or more combinations of biometric data and personal keys in an unprocessed and unencrypted form after the secondary data has been formed and prior to any storage, and stores the secondary data in the repository for subsequent use.

c. Referring to claim 30:

Please replace claim 30 as follows:

A computer readable storage device storing program instructions for execution by a computer, such that when the computer executes the program instructions, it performs a computer-implemented method for processing data, comprising:

(a) performing, in a computer, an enrollment process, comprising:

receiving a first biometric data and a first personal key;

processing the first biometric data combined with the first personal key through an irreversible cryptographic algorithm to form a first processed data comprised of the first biometric data and the first personal key in an irreversibly encrypted form;

eliminating all storage or trace of the first biometric data and the first personal key in an unprocessed and unencrypted form after the first processed data has been formed and prior to any storage; and

storing the first processed data in a repository for use in a subsequent authentication process; and

(b) performing, in a computer, an authentication process, comprising:

receiving a second biometric data and a second personal key;

processing the second biometric data combined with the second personal key through the irreversible cryptographic algorithm to form a second processed data comprised of the second biometric data and the second personal key in an irreversibly encrypted form;

eliminating all storage or trace of the second biometric data and the second personal key in an unprocessed and unencrypted form after the second processed data has been formed and prior to any comparison;

comparing the second processed data to the first processed data previously stored in the repository, without accessing either the first or second processed data in an unprocessed and unencrypted form, in order to enable authentication of the second biometric data and the second personal key in a confidential manner; and

generating a signal pertaining to the comparison of the second processed data to the first processed data for use in the authentication process.

d. Referring to claim 31:

Please replace claim 31 as follows:

The computer readable storage device of claim 30 further comprising generating a first variant from the first biometric data prior to processing the first biometric data and the first personal key through the irreversible cryptographic algorithm.

e. Referring to claim 32:

Please replace claim 32 as follows:

The computer readable storage device for performing the method of claim 30 further comprising generating a second variant from the second biometric data prior to processing the second biometric data and the second personal key through the irreversible cryptographic algorithm.

f. Referring to claim 33:

Please replace claim 33 as follows:

The computer readable storage device of claim 30 further comprising processing the first biometric data through a secondary irreversible cryptographic algorithm prior to processing the first biometric data and the second biometric data through the irreversible cryptographic algorithm.

g. Referring to claim 34:

Please replace claim 34 as follows:

The computer readable storage device of claim 30 further comprising adding salt to the first biometric data and the first personal key prior to processing the first biometric data and the second biometric data through the irreversible cryptographic algorithm.

h. Referring to claim 35:

Please replace claim 35 as follows:

The computer readable storage device of claim 30 further comprising processing the first personal key through a reversible cryptographic algorithm prior to processing the first biometric data and the first personal key through the irreversible cryptographic algorithm.

i. Referring to claim 36:

Please replace claim 36 as follows:

The computer readable storage device of claim 30 further comprising associating a first primary key to the first processed data.

j. Referring to claim 37:

Please replace claim 37 as follows:

The computer readable storage device of claim 30 further comprising associating a second primary key to the second processed data.

k. Referring to claim 38:

Please replace claim 38 as follows:

The computer readable storage device of claim 30 wherein receiving the first biometric data and the first personal key occurs during an enrollment process.

l. Referring to claim 39:

Please replace claim 39 as follows:

The computer readable storage device–of claim 30 wherein receiving the second biometric data and the second personal key occurs during an authentication process.

m. Referring to claim 40:

Please replace claim 40 as follows:

The computer readable storage device–of claim 30 wherein generating a signal includes issuing a confirmation signal when the second processed data matches the first processed data.

n. Referring to claim 41:

Please replace claim 41 as follows:

The computer readable storage device of claim 40 wherein issuing a confirmation signal allows access to a facility.

o. Referring to claim 42:

Please replace claim 42 as follows:

The computer readable storage device of claim 40 wherein issuing a confirmation signal allows access to a system.

p. Referring to claim 43:

Please replace claim 43 as follows:

The computer readable storage device–of claim 30 wherein generating a signal includes issuing a rejection signal when the second processed data does not match the first processed data.

q. Referring to claim 44:

Please replace claim 44 as follows:

The computer readable storage device of claim 30 further comprising storing the first processed data in a database.

r. Referring to claim 45:

Please replace claim 45 as follows:

The computer readable storage device of claim 44 wherein the database includes a plurality of first processed data.

s. Referring to claim 46:

Please replace claim 46 as follows:

A computer readable storage device storing program instructions for execution by a computer, such that when the computer executes the program instructions, it performs a method for processing data, comprising:

receiving biometric data and a personal key;

processing the biometric data combined with the personal key through an irreversible cryptographic algorithm to form a processed data comprised of the biometric data and the personal key in an irreversibly encrypted form;

eliminating all storage or trace of the biometric data and personal key in an unprocessed and unencrypted form prior to any comparison; and

comparing the processed data to secondary data stored in a repository, without accessing the processed data in an unprocessed and unencrypted form, in order to enable authentication of the biometric data and personal key in a confidential manner ;

wherein the secondary data comprises one or more combinations of biometric data and personal keys stored in the repository in an irreversibly encrypted form during an enrollment process that processes the one or more combinations of biometric data and personal keys through an irreversible cryptographic algorithm to form the secondary data, eliminates all storage or trace of the one or more combinations of biometric data and personal keys in an unprocessed and unencrypted form after the secondary data has been formed and prior to any storage, and stores the secondary data in the repository for subsequent use.

t. Referring to claim 47:

Please replace claim 47 as follows:

The computer readable storage device of claim 46 further comprising generating a variant from the biometric data prior to processing the biometric data and the personal key through the irreversible cryptographic algorithm.

u. Referring to claim 48:

Please replace claim 48 as follows:

The computer readable storage device of claim 46 further comprising processing the biometric data through a secondary irreversible cryptographic algorithm prior to processing the biometric data and the personal key through the irreversible cryptographic algorithm.

v. Referring to claim 49:

Please replace claim 49 as follows:

The computer readable storage device of claim 46 further comprising adding salt to the biometric data and the personal key prior to processing the biometric data and the personal key through the irreversible cryptographic algorithm.

w. Referring to claim 50:

Please replace claim 50 as follows:

The computer readable storage device of claim 46 wherein receiving the biometric data and the personal key occurs during an authentication process.

x. Referring to claim 51:

Please replace claim 51 as follows:

The computer readable storage device of claim 46 further comprising associating a primary key with the biometric data and the personal key.

y. Referring to claim 52:

Please replace claim 52 as follows:

The computer readable storage device of claim 46 wherein the secondary data includes a secondary biometric data and a secondary personal key.

z. Referring to claim 53:

Please replace claim 53 as follows:

The computer readable storage device of claim 52 wherein the secondary biometric data and the secondary personal key is received during an enrollment process.

aa. Referring to claim 54:

Please replace claim 54 as follows:

The computer readable storage device of claim 46 further comprising generating a signal corresponding to the comparison of the processed data to the secondary data.

bb. Referring to claim 55:

Please replace claim 55 as follows:

The computer readable storage device of claim 54 wherein generating a signal includes issuing a confirmation message when the processed data matches at least a portion of secondary data.

cc. Referring to claim 56:

Please replace claim 56 as follows:

The computer readable storage device of claim 54 wherein generating a signal includes issuing a denial message when the processed data does not match at least a portion of secondary data.

dd. Referring to claim 57:

Please replace claim 57 as follows:

The computer readable storage device of claim 54 wherein generating a signal allows entry into a facility when the processed data matches the secondary data.

ee. Referring to claim 58:

Please replace claim 58 as follows:

The computer readable storage device of claim 54 wherein generating a signal allows entry into a system when the processed data matches the secondary data.

Allowable Subject Matter

4. Claims 1-58 are allowed.

Conclusion

5. Any inquiry concerning this communication or earlier communications from the examiner should be directed to NIRAV PATEL whose telephone number is (571)272-5936. The examiner can normally be reached on 8 am - 4:30 pm (M-F).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/N. P./
Examiner, Art Unit 2435
/Kimyen Vu/
Supervisory Patent Examiner, Art Unit 2435